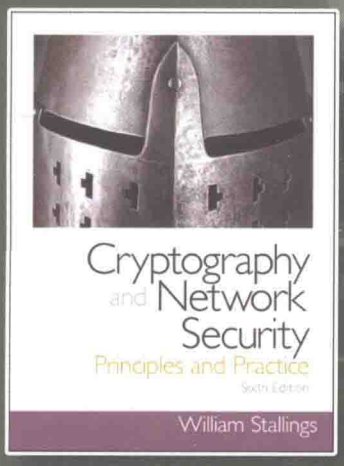
国外计算机科学教材系列

PEARSON

★William Stallings

密码编码学与网络安全
——原理与实践（第六版）

Cryptography and Network Security
Principles and Practice, Sixth Edition



[美] William Stallings 著

唐明 李莉 杜瑞颖 等译

张焕国 审校

中国工信出版集团

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

国外计算机科学教材系列

密码编码学与网络安全

——原理与实践(第六版)

Cryptography and Network Security

Principles and Practice, Sixth Edition

[美] William Stallings 著

唐 明 李 莉 杜瑞颖 等译

张焕国 审校

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书系统介绍了密码编码学与网络安全的基本原理和应用技术。全书的内容分为以下七个部分：对称密码部分讨论了对称加密的算法和设计原则；公钥密码部分讨论了公钥密码的算法和设计原则；密码学中的数据完整性算法部分讨论了密码学 Hash 函数、消息认证码和数字签名；相互信任部分讨论了密钥管理和用户认证技术；网络安全与 Internet 安全部分讨论了应用密码算法和安全协议为网络和 Internet 提供安全；系统安全部分讨论了保护计算机系统免受各种安全威胁的技术；法律与道德问题部分讨论了与计算机和网络安全相关的法律与道德问题。本书的第六版与第五版相比，书的章节组织基本不变，但增加了许多新内容。如增加了云安全、新 Hash 函数标准 SHA-3、真随机数产生器、移动设备安全等新内容。而且许多章节的论述方法也做了调整，使之更贴近技术实际，使读者更易理解。

本书可作为研究生和高年级本科生的教材，也可供从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

版权货号合同登记图图字：01-2013-6966

图书在版编目（CIP）数据

密码编码学与网络安全：原理与实践：第 6 版/（美）斯托林斯（Stallings, W.）著；唐明等译.
北京：电子工业出版社，2015.3
书名原文：Cryptography and Network Security: Principles and Practice, Sixth Edition
国外计算机科学教材系列
ISBN 978-7-121-24667-8

I. ①密… II. ①斯… ②唐… III. ①电子计算机-密码术-高等学校-教材 ②计算机网络-安全技术-高等学校-教材 IV. ①TP309.7 ②TP393.08

中国版本图书馆 CIP 数据核字（2014）第 254645 号

策划编辑：谭海平
责任编辑：李秦华
印　　刷：三河市华成印务有限公司
装　　订：三河市华成印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　　邮编：100036
开　　本：787×1092　1/16　印张：36　字数：1115 千字
版　　次：2003 年 11 月第 1 版（原著第 3 版）
　　2015 年 3 月第 4 版（原著第 6 版）
印　　次：2015 年 3 月第 1 次印刷
定　　价：79.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

"There is the book, Inspector. I leave it with you, and you cannot doubt that it contains a full explanation."

——*The Adventure of the Lion's Mane*, Sir Arthur Conan Doyle

第六版的新内容

在本书第五版出版后的4年中，该领域仍处于不断地发展变革之中。在这新版中，我试图在继续广泛涵盖本领域的主要内容的同时，增加这些新的变化。进行本次修订之初，许多讲授该课程的教师和研究该领域的专业人员都已经阅读过本书的第五版。这使得许多地方的叙述变得更清晰、更紧凑，对插图也进行了改进。

除了这些为改进教学法和使用户易读所做的修改以外，还有一些实质性的变化贯穿在本书中。与第五版相比，本书大体上保持了相同的章节，但修正了许多素材并增加了新的素材，最主要的变化包括以下几个方面：

- **网络访问控制**：新增加了关于网络访问控制的一章，包括对可扩展认证协议 EAP 和 IEEE 802.1X 的简介与讨论。
- **云安全**：新增加了关于云计算安全问题的一节。
- **SHA-3**：新增加了一节，介绍在2012年被采用的新的密码 Hash 函数标准 SHA-3。
- **密钥封装**：新增加了一节，介绍在许多应用中用以保护对称密钥的密钥封装。
- **椭圆曲线数字签名算法(ECDSA)**：新增加了一节介绍 ECDSA。由于 ECDSA 比其他数字签名方案更高效，它被越来越多的数字签名应用所采用。
- **RSA 概率签名方案(RSA-PSS)**：基于 RSA 的数字签名方案也许是使用最广泛的。新的一节介绍最近被标准化的 RSA-PSS，它正在替换基于 RSA 的旧方案。
- **真随机数发生器**：传统的真随机数发生器受限于它们的低位率，但是新一代的硬件真随机数发生器已经成为可用的。它在性能上已比得上软件伪随机数发生器。新的一节介绍真随机数发生器和英特尔的数字随机数发生器(DRNG)。
- **个人身份认证(PIV)**：NIST 发布了基于智能卡的用户认证标准集，这一标准集已开始被广泛使用。新增加了一节介绍 PIV。
- **移动设备安全**：移动设备安全成为企业网络安全的一个本质性问题。新增加了一节介绍移动设备安全。
- **恶意软件**：和第五版的恶意软件那章相比，本章关注的有所不同。相比于传统的病毒、蠕虫的直接感染，现在越来越多的后门/Rootkit 类恶意软件被社会工程攻击所安装，且网络钓鱼也比以前更多了。本版介绍了这些新趋势。
- **教学大纲样例**：本书包含多于一学期的内容，因此，为教师提供了若干教学大纲样例，以在有限的时间内(如16周或12周)使用本书。这些样例是基于使用第五版讲授的实际经验。

- **关于 Sage 的视频例子**：新的一版提供了许多关于 Sage 的视频教程，附录 B 介绍了 Sage。
- **学习目标**：每一章以一个学习目标列表开始。

本书的目标

本书的目标是概述密码学与网络安全的原理和应用。本书的前一部分给出关于密码学和网络安全的指导性概述。后一部分讨论网络安全的实际应用，包括已经实现或正用于提供网络安全的实用应用软件。

因此本书涉及多个学科。特别地，要想理解本书讨论的某些技术的精髓，必须要有数论的基本知识和掌握概率论中的某些结果。然而本书试图自成体系，不仅给出了必需的数论知识，而且让读者对这些知识有直观的理解。采用的方法是，在需要的时候才引入这些背景知识。这样有助于读者理解讨论这些背景知识的动机，作者认为这种方法比把所有的数学知识一次性全部放在本书开头要好。

ACM/IEEE 计算机科学课程 2013 的支持

本书适合于学术和专业人员使用。作为教科书，本书可作为计算机科学、计算机工程、电气工程专业本科生密码学与网络安全方面课程的教材，学时为一学期。本版的修订是为了支持当前草案版本的 ACM/IEEE 计算机科学课程 2013（CS2013）。CS2013 在课程体系中增加了 IAS（Information Assurance and Security）内容的课程，并将其作为计算机科学知识体系中的一个知识领域。CS2013 认为把 IAS 纳入课程体系，是因为 IAS 对于计算机科学教育具有关键作用。CS2013 把将所有课程分为三类：核心课程 1（课程应包含所有的课题）；核心课程 2（应包含全部或几乎全部的课题）；选修课程（根据意愿适当地提供广度与深度）。在 IAS 领域，CS2013 推荐把网络安全的基本概念纳入核心课程 1 和核心课程 2 中，而把密码学部分作为选修。本书实际上涵盖了 CS2013 所列举的三类课程中的所有课题。

本书还可用做参考用书或作为自学教材。

本书的组织

本书由以下七个部分组成（概览全貌请见第 0 章）：

- 对称密码
- 公钥密码
- 密码学中的数据完整性算法
- 相互信任
- 网络安全与 Internet 安全
- 系统安全
- 法律与道德问题

本书还针对教学的需要，提供了计算机代数系统 Sage 和大量图表使得表达更加清晰。每一章中都有关键术语、习题、思考题和推荐读物。本书还给出了术语表，常用的首字母缩略词表和参考文献。另外，对于教师还提供了试题库。

教学支持文档

本学科十分有趣而且发展迅速，本书的主要目的是为讲授这一学科内容提供一个有效的教学工具。该目的反映在本书的结构及支持文档。对于教师，我们提供了下列补充材料：

- **答案手册**：对于每章末尾的思考题和习题的答案。
- **项目手册**：对于下面列出的所有项目建议的任务分配方案。
- **PPT 幻灯片**：包含所有章节内容的幻灯片，适于讲课中使用。
- **PDF 文件**：本书中所有图和表的副本文档。
- **习题集**：按章的习题集和答案。
- **教学大纲样例**：本书包含多于在一学期讲授的内容，因此为教师提供了若干教学大纲样例，以指导在有限时间内使用本书。这些样例基于使用本书第五版的讲授实践经验。

在教师资源中心 IRC(Instructor Resource Center)中提供了所有的这些支持文档，可以通过出版商的网站：www. pearsonhighered. com/stallings 或点击本书网站 WilliamStallings. com/Cryptography 上的教师资源链接来获取。要想获取访问 IRC 的权限，请通过 pearsonhighered. com/educator/replocator/requestSalesRep. page 或者 Prentice Hall 的客服电话 1-800-526-0485 联系当地的 Prentice Hall 的经销商①。

在本书网站 WilliamStallings. com/Cryptography 上(点击教师资源链接)还包括以下资源：

- 链接到使用本书的其他课程的网站。
- 使用本书的教师邮箱列表，他们通过邮件互相讨论问题或对作者提出建议。

项目和其他学生练习

对许多教师来说，密码学或信息安全课程的一个重要组成部分就是制定一个或一系列项目使得学生有机会亲手实践，以加深对本教材中所学知识的理解。本书在很大程度上对该课程提供全面支持，包含了课程中一整套的项目组件。教师资源中心(IRC)不仅包括如何布置和构建项目，而且还包括一系列涵盖本书内容的推荐教学项目：

- **Sage 项目**：下一节中详细介绍。
- **黑客项目**：本项目的目的是阐明入侵检测和预防的关键问题。
- **分组密码项目**：本实验对 AES 加密算法的操作过程进行跟踪，手工进行一轮计算，并使用不同的分组密码工作模式进行计算。实验也包括 DES 算法。每种情况下都由在线(或离线下载)Java 小程序来实现 AES 或 DES 的运算。
- **实验室练习**：一系列针对本书里的概念进行编程和做实验的项目。
- **研究项目**：一系列指导学生研究 Internet 有关课题以及撰写研究报告的课外研究课题。
- **编程项目**：一系列涵盖大部分课程内容且可在任何平台上用任何适当的语言实现的程序设计项目。
- **安全评估实践**：用于检验已有组织机构的现有架构和实现的一系列活动。

① 为获取本书的教学支持文档，可参阅本书目录后所附的“教学支持说明”——编者注。

- **防火墙项目**：一个简易的网络防火墙可视化模拟器课题，用以支持讲授防火墙基本原理的练习。
- **案例研究**：一系列的实际案例研究，包括学习目标，案例描述，系列的案例讨论问题。
- **书面作业**：每一章里推荐了一些书面作业。
- **课外阅读/报告作业**：每一章在参考文献中都包含有论文列表，可让学生阅读并写出简短报告。

这些各种各样的项目和学生练习使得教师能够方便地使用本书，把它当做丰富多样的教学经验中的一个组件。从而可以方便地安排课程计划，以适应教师和学生的各种特殊需求。具体细节请参见附录 A。

Sage 计算机代数系统

本书的一个最重要的特色就是使用 Sage 实现密码算法示例和作业。Sage 是一个开源的、跨平台的免费软件包，它实现了一个强大的、灵活的、易学的数学和计算机代数系统。与 Mathematica，Maple 和 MATLAB 等系统不同，Sage 没有使用许可和使用费的限制。因此 Sage 可以在学校的计算机和网络上使用，学生也可以分别将其下载到他们自己的计算机上在家里使用。使用 Sage 的另外一个好处是学生可以掌握一个非常强大、灵活的工具来帮助计算解决几乎所有的数学问题，而不仅限于密码学。

在对密码算法数学基础的教学过程中，使用 Sage 能够显著增强教学效果。本书的附录 B 中提供了涵盖各种密码学概念的大量 Sage 示例。

附录 C 按照密码学概念的分类给出了习题集，它能够使学生得到关于密码算法的第一手经验。本书的教师资源中心 IRC 为教师提供了该附录。附录 C 中专门有一节介绍如何下载和使用 Sage，另一节介绍 Sage 编程基础，除此以外还包括为学生准备的以下分类习题：

- **第 2 章——古典密码**：仿射密码和 Hill 密码。
- **第 3 章——分组密码和数据加密标准 DES**：基于 SDES 的练习。
- **第 4 章——数论和有限域的基本概念**：欧几里得算法和扩展欧几里得算法，多项式算术，有限域 $GF(2^n)$。
- **第 5 章——高级加密标准 AES**：基于 Sage 的练习。
- **第 6 章——伪随机数发生器和流密码**：BBS、线性同余和 ANSI X9.17 伪随机数发生器。
- **第 8 章——数论入门**：欧拉函数，Miller-Rabin 测试，因子分解，模幂运算，离散对数，以及中国剩余定理。
- **第 9 章——公钥密码和 RSA**：RSA 加密/解密以及签名。
- **第 10 章——其他公钥密码体制**：Diffie-Hellman 密钥交换，椭圆曲线密码。
- **第 11 章——密码学 Hash 函数**：基于数论的 Hash 函数。
- **第 13 章——数字签名**：DSA。

提供给学生的在线文档

在这新的一版书中，两个网站为学生提供了大量在线原始支持材料。WilliamStallings.com/Cryptography 的合作网站(点击学生资源链接)包含一系列按章组织的章节和本书的勘误表。

购买新一版的书[①]可以获得6个月在线材料访问权限，包括以下内容：

- **在线章节**：为了减少本书(英文版)的篇幅和成本，书中的4个章节提供了PDF格式的电子文档，其中包括关于计算机安全的三章以及关于法律与道德的一章。在本书的目录中列出了这些章节。
- **在线附录**：支持材料包含了本书正文中涉及的大量有趣的话题，但在本书(英文版)纸质印刷版中没有提供。我们为对此感兴趣的学生们提供了包含了这些话题的总计20个在线附录。在本书的目录中列出了这些附录。
- **课后作业和答案**：为了帮助学生更好地学习和理解本书内容，我们单独提供了课后习题和答案集。
- **关键论文**：我们从专业文献中选择了一定数量的论文，其中许多是很难找到的。提供给读者进一步地阅读。
- **支持文档**：本书引用的其他各种类型的有用文档同时在线提供。
- **Sage代码**：附录B中给出了示例的Sage源代码。如果学生们想要实现这些示例，可以以此作为参考。

致谢

本次修改得益于许多人的审阅，他们花费了大量的时间和精力。下列这些人员审阅了所有或大部分手稿：Steven Tate(北卡罗来纳大学Greensboro分校)、Kemal Akkaya(南伊利诺伊大学)、Bulent Yener(伦斯勒理工学院)、Ellen Gethner(科罗拉多大学，丹佛分校)、Stefan A. Robila(蒙特克莱尔州立大学)以及Albert Levi(土耳其伊斯坦布尔的Sabanci大学)。

我还要感谢那些详细审阅其中某一章或数章的人员：Kashif Aftab, Jon Baumgardner, Alan Gantrell, Rajiv Dasmohapatra, Edip Demirbilek, Dhananjoy Dey, Dan Dieterle, Gerardo Iglesias Galvan, Michel Garcia, David Gueguen, Anasuya Threse Innocent, Dennis Kavanagh, Duncan Keir, Robert Knox, Bob Kupperstein, Bo Lin, Kousik Nandy, Nickolay Olshevsky, Massimiliano Sembiante, Oscar So, and Varun Tewari。

此外，我也有幸审阅了一些领域大师的研究成果，这些大师包括英特尔公司的Jesse Walker(英特尔的数字随机数发生器)、Vigil Security公司的Russ Housley(密钥封装)、Joan Daemen(AES)，圣克拉拉大学的Edward F. Schaefer(简化的AES)、前RSA实验室的Tim Mathews(S/MIME)、滑铁卢大学的Alfred Menezes(椭圆曲线密码学)、*The Cryptogram*一书的编辑与发行人William Sutton(古典密码)、约翰·霍普金斯大学的Avi Rubin(数论)、信息安全公司的Michael Markowitz(SHA和DSS)、IBM因特网安全系统部的Don Davis(Kerberos)、BBN科技公司的Steve Kent(X.509)和Phil Zimmerman(PGP)。

Nikhil Bhargava(IIT Delhi)开发了一系列的在线家庭作业和解答。微软和华盛顿大学的Dan Shumow开发了附录B和附录C中所有的Sage示例和作业。达科他州立大学的Sreekanth Malladi教授开发了黑客练习。澳大利亚国防学院的Lawrie Brown提供了AES/DES分组密码项目和安全评估练习。

Purdue大学的Sanjay Rao和Ruben Torres为教师资源中心(IRC)的实验室练习做了很多工

① 仅指在美国销售的原英文版——编者注。

作。下列人员为教师资源中心的项目计划做了许多工作：Henning Schulzrinne(Columbia 大学)，Cetin Kaya Koc(Oregon 州立大学)和 David Balenson(Trusted Information Systems and George Washington University)。Kim McLaughlin 提供了习题库。

最后，还要感谢负责本书出版的工作人员，他们都做得很优秀。包括培生教育出版集团的工作人员，特别是责任编辑 Tracy Johnson，助理编辑 CaroleSnyder，产品监督 Robert Engelhardt，产品项目经理 Pat Brown。我还要感谢 Shiny Rajesh 和 Integra 出版社的其他员工的出色和快捷的工作。还要感谢培生教育出版集团的市场和销售工作人员，没有他们的努力，这本书就不可能摆在你的面前。

在这么多帮助面前，我几乎没有什么可以居功自傲的。但我可以自豪地说，即使没有这些帮助，我也会选择所有这些内容。

作者简介

William Stallings 编写出版了 17 部著作，经修订再版累计 40 多本关于计算机安全、计算机网络和计算机体系结构等领域的书籍。他的著作无数次出现在出版物中，包括 *Proceedings of the IEEE*、*ACM Computing Reviews* 和 *Cryptologia*。

他 11 次获得美国“教材和著作家协会”(Text and Academic Authors Association) 颁发的“年度最佳计算机科学教材”奖。

在过去的 30 年中，他曾在该领域的数个高科技企业中担任技术骨干、技术管理者和技术执行领导。他设计和实现了适用于从微型机到大型机的各种类型的计算机、操作系统的基于 TCP/IP和基于 OSI 的协议。目前，他作为独立顾问为政府机构、计算机硬件制造商、软件开发商以及广大用户提供包括设计、选择和使用网络软件和产品的咨询服务。

他建设并维护了计算机科学专业学生资源网站 WilliamStallings. com/StudentSupport. html。该网站提供为计算机科学专业的学生(和专业人员)提供各种文档和链接。他是 *Cryptologia* 杂志的编委，该杂志是密码学的学术期刊。

William Stallings 博士先后获得了 Notre Dame 电气工程学士学位和 MIT 计算机科学博士学位。

PEARSON

北京培生信息中心
北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 1208 室
邮政编码：100013
电话：(8610) 57355171/57355169/57355176
传真：(8610) 58257961

Beijing Pearson Education
Information Centre
Suit 1208, Tower D, Beijing Global Trade Centre,
36 North Third Ring Road East,
Dongcheng District, Beijing, China 100013
TEL: (8610)57355171/57355169/57355176
FAX: (8610)58257961

尊敬的老师：

您好！

为了确保您及时有效地申请教辅资源，请您务必完整填写如下教辅申请表，加盖学院公章后将扫描件用电子邮件的形式发送给我们，我们将会在 2-3 个工作日内为您开通属于您个人的唯一账号以供您下载与教材配套的教师资源。

请填写所需教辅的开课信息：

采用教材			□中文版 □英文版 □双语版
作　　者		出版社	
版　　次		ISBN	
课程时间	始于　　年　　月　　日	学生人数	
	止于　　年　　月　　日	学生年级	□专科　　□本科 1/2 年级 □研究生　　□本科 3/4 年级

请填写您的个人信息：

学　　校			
院系/专业			
姓　　名		职　　称	□助教 □讲师 □副教授 □教授
通信地址/邮编			
手　　机		电　　话	
传　　真			
official email(必填) (eg:XXX@ruc.edu.cn)		email (eg:XXX@163.com)	
是否愿意接受我们定期的新书讯息通知：　　□是　　□否			

Publishing House of Electronics Industry
电子工业出版社：www.phei.com.cn
www.hxedu.com.cn
北京市万寿路 173 信箱高等教育分社（100036）
联系电话：010-88254555
E-mail：Te_service@phei.com.cn

系 / 院主任：_____（签字）

（系 / 院办公室章）

_____年_____月_____日

目　录

第一部分　对 称 密 码

第二部分　公钥密码

第三部分　密码学中的数据完整性算法

在 线 部 分

第六部分　系 统 安 全

第七部分　法律与道德问题